

# **Distributed Security Architectures**

## **First Quarter 2004 Progress Report**

**Covers work done October through December, 2003.**

### **Personnel:**

**Staff:** Mary Thompson, Abdelilah Essiari

### **Akenti Policy Engine**

Added the code to support unchecked policy collection on the sever side. This code follows the same procedures as a check access call but does not stop when a policy or use-condition cannot be found or fails to verify. It continues to find all available policy and returns a status code indicating the reason for failure for any certificate that can not be verified. It is intended to be used by stakeholders to verify that the policy they have written for a resource is correctly formatted, consistent and valid.

### **Certificate Generators**

Tested out the policy collection GUI once the code supporting it in the policy engine was finished. Demonstrated the interface as SC03 as part of the Distributed Security demo. Tested it on Windows as well as the Unix platforms.

### **Code Distribution**

Updated only for a few bug fixes.

### **Collaboration with Other Projects**

Work with the SciShare project led to the development of a customized graphical interface to chose a policy for a set of files. Rather than using the standard Akenti certificate generators that create policy by writing Akenti policy, use-condition and attribute certificates, the SciShare interface allows a provider of files to choose if they are to be shared for writing or only for reading and what groups will be allowed access. Then the Akenti certificates are written behind the scenes without the stakeholder having to learn how Akenti stores policy, thus greatly simplifying his understanding of policy. Since the policy requirements of SciShare are relatively simple, they can be represented by a few menu choices. The underlying assumptions are that there will be only one authority writing policy and assigning attributes for a given resource, all the policy will be stored in a pre-configured place, and unconditional read or write access to one or more groups is all that is required.

This interface was demonstrated at SC03 as part of the SciShare demo. The Fusion Grid people were interested in experimenting with a similar interface for their remote job submission authorization policy. We now plan as part of our future work to design a simple standalone policy interface for simple policies. Our first customer will be the FusionGrid.

We started collaborating extensively this quarter with the National Internet Measurement Infrastructure (NIMI) NSF project. They are using Akenti to authorize the uploading and execution of measurement probes at distributed sites. We started by helping them build and install our software on their NetBSD machines. Once they were able to call the Akenti libraries from their code, we advised them about their policy design. NIMI is using our code in the push model, where the client first contacts a site-central point of contact (CPOC) and requests authorization for an action. The client program gets back a capability certificate signed by the CPOC which it presents to several hosts at that site to start measurements.